Strategy Research Project

ENABLING MISSION COMMAND THROUGH CYBERPOWER

BY

COLONEL KENNETH A. LENIG
United States Army

USAWC CLASS OF 2011

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 22-03-2011	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE Enabling Mission Command Through Cyberpower	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Colonel Kenneth A. Lenig	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Colonel John H. Greenmyer III	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This Strategic Research Project (SRP) examines the current and future construct and requirements of the United States Army's mission command concept and identifies the necessary cyber capabilities to meet these requirements and enable this concept. This examination reviews the current and future cyber threat, the concept of mission command, and the importance of cyberpower in its role as both a protector and enabler of mission command. Further, it provides a detailed look at the organization, material, and personnel postured to provide these capabilities. It continues with an examination of critical linkage and collaboration between DoD, the Services, the interagency, Department of Homeland Security, industry, and our coalition partners. Finally, it provides recommendations for consideration throughout the paper which address identified gaps and challenges. Mission command is the Army's commander-centric concept which depends upon cyberpower and supporting net-centric, cyber security capabilities. Cyberpower serves as the great enabler for the mission commander at the strategic to tactical level both today and for the future.

15. SUBJECT TERMS
Mission Command, Cyberpower, Information Technology

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	28	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

ENABLING MISSION COMMAND THROUGH CYBERPOWER

by

Colonel Kenneth A. Lenig
United States Army

Colonel John H. Greenmyer III
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of iol*the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. ARMY WAR COLLEGE
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Kenneth A. Lenig

TITLE: Enabling Mission Command through Cyberpower

FORMAT: Strategy Research Project

DATE: 22 March 2011 WORD COUNT: 5,380 PAGES: 28

KEY TERMS: Mission Command, Cyberpower, Information Technology

CLASSIFICATION: Unclassified

This Strategic Research Project (SRP) examines the current and future construct and requirements of the United States Army's mission command concept and identifies the necessary cyber capabilities to meet these requirements and enable this concept. This examination reviews the current and future cyber threat, the concept of mission command, and the importance of cyberpower in its role as both a protector and enabler of mission command. Further, it provides a detailed look at the organization, material, and personnel postured to provide these capabilities. It continues with an examination of critical linkage and collaboration between DoD, the Services, the interagency, Department of Homeland Security, industry, and our coalition partners. Finally, it provides recommendations for consideration throughout the paper which address identified gaps and challenges. Mission command is the Army's commander-centric concept which depends upon cyberpower and supporting net-centric, cyber security capabilities. Cyberpower serves as the great enabler for the mission commander at the strategic to tactical level both today and for the future.

ENABLING MISSION COMMAND THROUGH CYBERPOWER

> America's digital infrastructure is critical to laying the foundation for our economic prosperity, government efficiency, and national security."
>
> —President Barack Obama
> Presidential Proclamation of National Cybersecurity Awareness Month[1]

The above statement from the full proclamation by President Obama serves as the starting point for this review and analysis of the cyber domain, cyberpower and its criticality, and in turn, its relationship to the Army concept of mission command.

The nature of current warfare stands as a distant cry from the age of traditional, industrial, and state-versus-state struggles. The world has undergone a global transformation. Today's security environment has become one where counter-insurgency, operations other than war (OOTW), and war not only between but also within nations, have become the norm. This emerging period of enduring and persistent conflict reinforces the criticality of command, control, and information on the battlefield and the importance of a new dimension of warfare – the cyber domain.

During the same time it takes for a human eye to blink, a message from a computing device can travel around the world! This message could transmit a harmful computer virus, a malicious code, or a rallying cry within or among belligerents (or potential ones). The importance of control, or at least management, of the internet and our supporting and supported military networks has not been more critical than it is today. In the future this criticality will only increase.[2]

The threat to our cyber systems is tangible and real. Hundreds (perhaps thousands) of intelligence agency operatives, foreign powers, non-state actors, or novice hackers stand active and ready to effect, influence, or otherwise adversely impact not only the military element of our national power but each and every one of the others.[3] Other countries aggressively aim to seize or manipulate the cyber environment to gain a strategic, operational, and tactical edge.

Cyber-warfare serves as an especially attractive and cost effective option to our adversaries, due mainly to its relative low cost when compared to expensive weapon system and costly increases in force structure. Cyber-warfare provides a cheap way to inflict significant damage. It only requires a few talented programmers to discover and exploit network vulnerabilities and rapidly cripple entire information systems upon which our military commanders and staffs depend.[4]

Throughout history smaller armies have attempted to confuse their enemies, disrupt or alter their strategic and operational plans, destroy their communications capabilities, and ultimately, gain peer-level status (if only for a brief period) with their stronger, more powerful foe. The birth of the cyber age provides the smaller less powerful adversary a new way to gain that advantage.

Essentially, two critical factors have raised the stakes in today's cyber struggle. These factors are information technology (IT) dependence and the rapid advance of IT capabilities. At both the tactical and operation levels, the United States' increased dependence upon modern information technology has created an environment where networks and information systems not only provide needed capabilities but also exploitable vulnerabilities.[5] Next, as the United States and our partners continue to evolve and transform, we have become even more dependent on an interconnected, yet increasingly vulnerable, global information grid (GIG). In order to effectively function, the US military, in fact all elements of national power, depend upon an available and secure GIG.[6]

This globally interconnected and mutually dependent grid introduces a relatively new strategic target. Interrupted cyber capabilities, even for a moment, can place our nation at risk of being effectively paralyzed.[7] In many cases, this paralysis can be achieved by relatively inexpensive and arguably rather subtle means. The stark reality is that the possibility to wreak havoc within our information environment is indeed possible, if not likely. Today's world stands at risk to be made chaotic without the use of any means of kinetic warfare. This opportunity to disrupt without risk makes cyber attack the potential warfare means of choice.[8] This reality makes cyber power an increasingly greater element to consider and plan for within our construct of national interests, strategy, and objectives.

Purpose

In general terms, this paper examines the dependent relationship between mission command and cyber power. It contends that the concept of mission command is not only enabled by cyber power but it is also protected by cyber security. To facilitate understanding of today's cyber world and its impact, an informative review of the current status for the key elements of the cyber domain and the concept of mission command will be explored. Next, how the Department of Defense (DoD) is organizing to protect and enable our efforts in the cyber domain will be reviewed. Further, a quick look at some of the key, critical enablers which promote cyberpower and cyber security is included. Finally, the direct and dependent relationship between cyberpower and mission command will be examined. Overall, this paper will demonstrate that mission command is a commander-centric concept which depends upon net-centric capabilities and cyber security.

What is Mission Command?

The concept of mission command appears new, but in actuality, the general concept is not wholly new at all. Despite recent proclamations and it being cast by much of the strategic leadership as revolutionary, the basic idea is derived from Prussian term –auftragstaktik."[9] Auftragstaktik, as an approach to warfare, focuses on mission-type orders and emphasizes the importance of clear and well understood commander's intent. This approach depends upon every Officer, NCO and Soldier understanding the senior commander's stated objectives and the role which they serve in achieving these objectives. Initiative is another critical aspect of auftragstaktik. This concept expects subordinates to seize and apply initiative confidently in pursuit of the commander's intent.[10]

In this manner, mission command is derived from auftragstaktik and, in many ways, already a part of our Army's mantra. Most of our Army already possesses a strong understanding of and recognized need for unity of effort, commander's intent, and initiative. However, auftragstaktik only begins to characterize today's concept of mission command. This new mission command is evolutionary and fully enabled via technology and cyber dominance.

Specifically, a command style which is decentralized, a command environment which empowers subordinates and subordinate commands, systems and critical thinking capabilities which promote increased decision-making tempo and responsiveness, units and leaders at all levels that are technically and tactically versatile and empowered to seize initiative represent the key elements of mission command. In its raw and truest form, the mission command approach informs subordinates what ends are to be achieved but not the specific execution ways to achieve them. The method is left to the subordinate leaders to determine.

To begin, mission command depends upon a clear understanding of commander's intent and nesting of intent across all levels of the command. Next, a mutual understanding of the expected desired effects of subordinates and subordinate organizations makes the commander's intent tangible and measurable. The true trademark of mission command is capable leadership at all levels which interacts clearly and often to integrate and synchronize the entire organization's effort both vertically and horizontally within the organization and, as required, across the interagency.[11]

Doctrinally, mission command has become the emerging multi-component, multi-layered, and multi-faceted construct which integrates the functions, techniques, and procedures of both the creative and cognitive parts of command.[12] The recently released Training and Doctrine Command Pamphlet 525-3-3 (U.S. Army Functional Concept for Mission Command) defines mission command as the authority and method where the commander uses ~~th~~e art of command and the science of control to integrate warfighting functions."[13] This definition represents a dramatic shift and growth from previous Army doctrine's characterization of mission command as the conduct of military operations through only objective-focused mission orders and decentralized execution. This shift also moves mission command well beyond Prussian auftragstaktik. The three key terms in this new definition are command, control, and integrate. Indications are that this new definition will be incorporated into the next version of Army Field Manual (FM) 3-0 (Operations).

The United States Army is not the only military which has embraced the concept of mission command. The British military employs a type of mission command as their primary method of decision-making and decision implementation. They promote decentralization of decision authorities and, in turn, empower individual leaders to seize initiative and then respond rapidly and appropriately to emerging situations without having to wait for decisions from higher commands. From the British Army's Doctrine Publication, mission command is comprised of ―timely decision-making, understanding a superior commander's intention, and a clear responsibility to fulfill that intention."[14] The last portion of this stresses the most significant element of British mission command – a requirement to fulfill that intention. This is reinforced by British doctrine, it is ―the fundamental responsibility to act (or, in certain circumstances, to decide not to act) within the framework of the commander's intentions."[15]

So what makes mission command any different from other styles or approaches to command? What makes it better suited to the volatile, uncertain, complex and ambiguous (VUCA) environment of today and tomorrow? The mission command concept links the critical, technical operations of electronic warfare, cyber security, intelligence, and communications.[16] It requires integration with information operations and it supports and integrates all of the warfighting functions. Mission command represents the fundamental and authoritative power to adjudicate issues which involve all of these areas. The Army views this new mission command as ―the integrating function that effectively combines all warfighting functional capabilities."[17]

The Key Elements of Mission Command

―In mission command, the commander is the central figure, and new responsibilities require a broader, more mission-oriented command structure."[18] said

Lieutenant General Robert Caslen, Commander of the Combined Arms Center (CAC) at Fort Leavenworth, Kansas (and also home of the U.S. Army's Mission Command Center of Excellence). Most students of the military recognize the importance of the command and control functions of a military commander. Mission command takes the concepts of command and control to another level.

Two newly emphasized features of mission command are the idea and application of the *art of command* and the *science of control*. The art of command and the science of control first appeared in Army doctrine in 2003.[19] Art is ~~a~~esthetic human output characterized by the skillful and creative application of principles."”[20] The commander is charged to meet certain responsibilities as part of the art of command. These new command responsibilities include understanding, visualizing, describing, directing, leading and assessing. They also demand effective team building; joint, coalition, and interagency partnership development; establishment of consistent strategic themes and communications; and engagement with all key players. This new construct uses the art of command as the *driver* for the science of control. The science of control includes planning, rehearsing, executing, and assessing operations and their respective effects.[21] Science focuses upon knowledge gained by skillful observation and collection coupled with refinement of information which has been compiled, fused, and displayed to enable improved understanding and decision-making and mission accomplishment.[22] The impact of cyberpower serves as the prevailing source for the *science of control* portion of the mission command construct.

The art of command and the science of control will lead to successful operations across the full-spectrum of possibilities via a clear understanding of the operational environment and by maintaining a necessary degree of operational adaptability. Mission command enables this enhanced operational adaptability by building adaptive teams which anticipate future change states and key decision points where changes-of-state matter the most. They accept risk to create opportunity, and expertly employ the power of information as an influencing activity.[23]

The term *battle command*, which did include both the aspects of art and science, has not been formally removed from the Army vernacular but has conceptually been subsumed by mission command. Army doctrine defines battle command as the –art and science of decision-making and leading to successfully accomplishing the mission.”[24] A reasonable and legitimate argument presents the idea that battle command had become overly system-centric while mission command is commander-centric with the art of command better enabled by robust networks and agile systems (science of control).

The Army has described mission command in a new way yet it desires to keep those parts that are time-tested and battle-proven. It also aims to include the ideas of better adaptation and more effective integration, both within the Army and with its partners. Further, the Army wants the new mission command to capture five primary sub-elements. First, mission command includes all the pertinent battle command ideas and calls for an adaptation of the operations process. Second, mission command depends upon operational design and operational art expertise. Next, mission command subsumes the command and control warfighting function while modifying it to be more relevant and coherent in joint, interagency, intergovernmental, and multinational processes and environments. Fourth, it stresses the empowerment of subordinates and the overall decentralization of operations. Finally, mission command is commander-centric where cyberpower supports the art of command and enables the science of control.

The Roles of Cyberpower

Mission command is dependently linked to cyberpower due to its enabling effect. Cyberpower provides the critical transmission layer, authoritative data and consistent databases, and automated analysis and decision tools which enables effective mission command to be realized.

Achieving the necessary and delicate balance between information access for those with the greatest need and the critical requirement to protect information and the information element is the paramount challenge to operations in the cyber domain. Cyberpower is achieved through both enabling and protecting both the cyber environment and the contents and mechanisms within that environment.

Cyber attacks occurred in the past and the threat for new and more sophisticated attacks in the future is growing.[25] Attacks of this sort can inflict great damage and can be launched by nations, terrorists, criminal gangs, or belligerent individuals. The concept of mission command depends on the ability to thwart or reduce the impact of these attacks and limit the associated degradation of network services, data integrity, and data accuracy.

Again, the two primary benefits cyberpower presents to mission command are its protection and enabling properties. Each will be examined in the next sections.

Enabling Mission Command with Cyberpower

Because mission command crosses and integrates the critical warfighting areas of electronic warfare, intelligence, communications, and information operations, the success of mission command is directly related to, and ultimately dependent upon, cyberpower. Absent the presence of legitimate and tangible cyberpower, the new concept of mission command cannot be realized.

Cyberpower depends directly upon resources that involve the creation, control, and communication of electronic and computer-based information. These resources include the communications infrastructure (or GIG), networks, software applications, and human skills. Cyberpower includes the internet of networked computers, but also intranets, cellular technologies and space-based communications. Cyberpower is the ability to produce better decisions, and subsequently obtain more preferred outcomes, through application of interconnected resources of the cyber domain. Basically, cyberpower enables mission command by creating friendly advantages, either through influence or action (or both), in each of the other domains (land, sea, air, space). Cyberpower enables mission command by producing preferred outcomes in the cyber domain and by applying information technology (IT) to gain preferred outcomes in those other domains. To achieve cyberpower and fully enable mission command, our forces need to control access to the domain while ensuring our freedom of action within that domain.[26] In this manner, cyber dominance is similar to air or sea superiority. The key remains the right balance between control and freedom.

To achieve cyberpower, and ultimately to become cyber dominant, not only must our nation and our military keep adversaries in a position of risk within the cyber domain but we must also maintain our freedom of maneuver. Creation of this delicate balance is the key factor in achieving cyber domain dominance and via fully supported mission command, can result in advantage, even dominance, in the other domains of land, air, sea, and space.

Protecting Mission Command with Cyberpower

During the American Civil War, dismounted units covered up to 20 miles a day to attack. During World War II, aircraft conducted strategic bombing raids in Europe and the Pacific in hours. During the Cold War, intercontinental missiles had the ability to attack targets in mere minutes. Today, cyber attacks can be initiated and achieve drastic, potentially catastrophic results in only seconds! Further, the speed of cyber attacks when coupled with their potential for relative anonymity within cyberspace gives a tremendous advantage to the offender. Finally, the attacker's offensive advantages do not remain stagnant. Offenders continue to develop and refine hacking tools making them cheaper to build, easier to employ, and able to cause greater damage.

To counter this threat, the U.S. military must be able to anticipate (even predict) attacks and ultimately be ready to defend our critical information infrastructure even faster. Response and reaction times need to be almost instantaneous! Cyber protection needs to be active, rapid, and even anticipative to effectively enable continuous and comprehensive mission command.

The Defense Department operates over 15,000 computer networks spanning 4,000 military posts, camps, and stations worldwide.[27] On a typical day in DoD over seven million computers and telecommunications tools are used across the globe employing thousands of military applications and software.[28] All of this makes the number of potential vulnerabilities staggeringly vast.

Protection of our cyber networks requires vigilance and preparedness to provide near real-time reaction to either stop cyber attacks before they are initiated or to effectively limit the damage inflicted. To be dominant in the cyber domain, the DoD needs to develop comprehensive strategies and policies and provide needed authorities and capabilities to those charged with defense and overall management of its information networks and data repositories. Absent a comprehensive cyber protection strategy and necessary resources (people, capabilities, and dollars), Army mission command is placed at risk. According to Melissa Hathaway, the Cybersecurity Chief at the National Security Council, ―protecting cyberspace requires strong vision and leadership and will require changes in policy, technology, education, and perhaps law."[29]

Critical DOD Efforts to Protect and Optimize the Cyber Domain

The DoD has begun a number of initiatives to respond to these challenges and to build its capabilities to promote and protect the cyber domain. DoD recognizes the importance of developing a comprehensive overall approach to cyberspace operations, looks to build greater cyber expertise and experience, aims to build new relationships and improve existing ones in the interagency and with other governments and militaries, and is centralizing cyberspace space command and control through the creation of the United States Cyber Command.[30]

The first effort involves the development of a comprehensive DoD approach. A comprehensive approach will help enable a secure cyber environment and provide the necessary priorities to plan, operate, and protect within this domain. Strategy and policy would codify this approach while promoting the concepts of layered cyber defense, network resiliency, self-healing, and data integrity. These concepts will provide the necessary confidence in cyberspace activities and promote mission command.

A supporting component of this new comprehensive cyber approach depends upon organizational and cultural changes in both the Army and DoD. To realize tactical, operational, and even strategic advantage, the Army and DoD need to build upon their recent efforts and continue to transform how they plan for the cyber domain, how they conduct network operations, how their forces are structured, and how they relate and collaborate within the DoD, between Services, with the interagency, industry, and our coalition partners.

Next, to realize cyberpower and provide 21st century mission command, the Army needs to emphasize, develop, and reward greater cyber expertise within its ranks. This expertise includes the average information technology (IT) user in addition to those professionally focused on IT and IT security. The Army needs to provide personnel with more information about cyber threats and institute more effective training to give them the skills needed to counter threats and reduce vulnerabilities. Both the Army and DoD need to do more to achieve these objectives. They each need to recognize that it can no longer have individual IT users who only think of the cyber domain as something that is just there for them to do their respective jobs. They need to employ an approach which creates and reinforces a sense of ownership and protection within their organizations.

The DoD has taken the lead in this protection effort. They aim to create this sense of ownership and protectorship of the cyber domain. DoD wants to cement its positive influence on users and organizations through education and accountability. The DoD and the Army have enacted inspection and monitoring programs which will discover violations and potential compromises and look to methods which hold leaders, personnel, and organizations accountable for security violations. To make this all possible, the DoD and our Army needs to grow in volume and mature in expertise. This growth and development needs to include both the cyber cadre and the cyber warrior. Investments in the human dimension will reap the greatest and most enduring rewards.

The next required critical effort involves improved interagency and international partnerships. The inherent interdependence of the cyber environment and the dependence of DoD networks upon commercial infrastructure forces collaboration across Service, department, agency, corporate, and even international boundaries. The recent WikiLeaks issue may deter information sharing and security collaboration with our coalition partners and allies. However, Robert J. Butler, Deputy Assistant Secretary of Defense for Cyber and Space Policy, reaffirmed that information sharing will continue within DoD, with our coalition partners, and also within the interagency. Butler stated that the DoD policy will institute more controls to relieve the ~~t~~ension between the strategy of share to win and the necessity to enforce need to know."[31]

The efforts of both DoD and the Army support the goal of a layered defense in depth through their coordination and synchronization of cyber defense. Specifically, coordination, collaboration, and integration needs to be sure to include law enforcement, defense support to civil authorities (DSCA), and homeland defense. Close coordination between the Department of Homeland Security (DHS) and DoD is especially important as these two are responsible for the majority of the cyber security effort. A recently signed agreement (September 2010) postures each of these organizations to collaborate and better meet their mutual missions of homeland security and homeland defense. The agreement created the framework for DHS, the National

Security Agency (NSA), and USCYBERCOM to better work together on issues in the cyber domain. This framework formalized a relationship which had been informal, inconsistent, and ad hoc.[32]

The last critical effort is the command of cyber operations. Secretary of Defense (SECDEF) Robert Gates formally established the United States Cyber Command (USCYBERCOM) on 23 June 2009. USCYBERCOM was designated a sub-unified command and fell under the direction of the United States Strategic Command (USSTRATCOM). USCYBERCOM was established to “plan, coordinate, integrate, synchronize, and conduct activities to (defend) specified DoD information networks and to conduct full spectrum military cyberspace operations to enable actions in all domains” and ensure our “freedom of action in cyberspace and deny the same to our adversaries.”[33]

As demonstrated by its mission statement, the directed focus of USCYBERCOM is the “fusion of all DoD cyberspace operations and contingency planning to coordinate and integrate a layered defense of DoD networks.”[34] The command will bring together current cyberspace resources, create a new synergy by fusing these resources, and synchronize efforts to defend the cyber environment. USCYBERCOM provides centralized command of cyber operations and defense, strengthens cyberspace capabilities across the DoD and within each Service, and integrates DoD’s cyber efforts with the other elements of national power. By doing these things, USCYBERCOM should improve the DoD’s ability to provide needed information and communication networks, effectively counter and ultimately defeat the growing cyber threat, maintain necessary database and associate data integrity, and provide overall assured access to and critical flexible maneuver within the cyber domain.[35]

The formulation of this command (and its supporting Service Component Commands (SCC) – the Army Service Component Command (ASCC) is United States Army Forces Cyber Command (USARFORCYBER)) represents the most recent, and arguably strongest, DoD organizational initiative in direct response to this ever-increasing threat to our nation, the military, other government, and commercial networks, information systems, and other command and control (C2) architectures. USARFORCYBER is focused solely on cyber and was recently formed at Fort Belvoir, Virginia.[36]

Critical Cyber Enablers

In addition to a comprehensive cyber approach, greater IT expertise, user-ownership of IT networks and systems, cyber partnerships within and beyond DoD, and centralized command of DoD cyber operations via USCYBERCOM, there exist a number of other critical items which enable and promote U.S. cyber dominance. The first of these is Strategic Battle Command (SBC).

According to the Army's Program Manager (PM) for Battle Command, SBC is a component of the Army Battle Command System (ABCS) and provides a system to enable Army and Joint commanders to report readiness, project their forces, and gain greater situational awareness. Strategic Battle Command provides operational and strategic tools to prepare the Army to bring the right forces, with the right capabilities, to the right fight, at the right time.[37] SBC includes these systems: Global Command and Control System – Army (GCCS-A), Defense Readiness Reporting System – Army (DRRS-A), and Net Enabled Command Capability (NECC).

The Global Command and Control System – Army (GCCS-A) serves as the Army's primary means of strategic, theater, and even tactical command and control. Largely the most important Army Battle Command System (ABCS) supporting the SBC, GCCS-A supports the full spectrum of military operations and provides the critical link for operational information and critical data between the strategic Global Command and Control System – Joint (GCCS-J) and the Army. GCCS-A contributes to mission planning, deployment support, operations, and redeployment. It provides a common operational picture (COP) of tactical level Army operations to Joint and Coalition partners and also provides total asset visibility to the Army. GCCS-A serves as the Commander's command system of choice for force planning and projection and situational awareness (SA). It is also the Army's system of record message traffic in the theater of operations and world-wide.[38]

The classified and web-based application which provides a timely and accurate monthly snapshot of specific and overall unit readiness is the Defense Readiness Reporting System – Army (DRRS-A). DRRS-A captures, compiles, and portrays mission critical information and readiness statuses in the areas of personnel or manning, individual and unit training readiness, and equipment readiness and availability. DRRS-A also supports the GCCS-A force readiness application. This keeps readiness data both accurate and common across the Army's network.

Net Enabled Command Capability (NECC) is the third important system supporting strategic battle command. NECC serves the DoD as its primary Joint command and control capability focused on providing the warfighting commander the necessary data and information infrastructure to make informed decisions that are timely and effective.[39]

Another critical enabler of cyberpower is the Warfighter Information Network – Tactical (WIN-T). WIN-T provides the Army with a high capacity communications network which links the tactical commander with higher level commanders and the Global Information Grid (GIG).[40] The GIG is DoD's worldwide network- centric information system. LandWarNet serves as the critical piece of WIN-T. LandWarNet represents the Army's primary effort to transform into a joint, net-centric, knowledge-based land power. It provides the common operational picture (COP) to the combatant commander through satellite, high capacity land-based radio systems, and network management all aimed at keeping the land forces connected, communicating and synchronized.[41]

This paper would be remiss if it failed to recognize the critical importance of firewalls, encryption, and intrusion-detection devices in the battle for cyber security. It is also important to note that recently DoD will increase cyber security across all the Services by increasing funding by $8 billion to $12 billion over the next five years.[42]

The last, and most critical enabler for cyberpower, is tactically adept, technically astute, and operationally proficient cyber-warriors. Jim Gosler, a veteran of the Central Intelligence Agency (CIA) and the National Security Agency (NSA), believes there are only approximately 1,000 people in the U.S. with the cyber defense skills needed and that up to 30,000 personnel are actually required.[43] These cyber-warriors must be capable of leading units which provide the important elements necessary for effective mission command in the current and future operating environment.

Cyber warriors are leaders and operators who make commander-centric operations (and mission command) possible by providing the tactical, operational, and strategic commanders with the ability to acquire and use the most critical and timely information; to fully visualize and, in turn, comprehend their specific battle environment; to coordinate and synchronize operations on land, air, sea, and space; and to integrate pertinent operations and supporting operational plans across all the elements of national power. The cyber warrior of today and tomorrow must fully understand the technical capabilities and limitations of their units and systems and be able to effectively describe these capabilities and limitations to their supported commanders. Thorough, and even anticipatory planning and flexibility to overcome the unexpected, are other important characteristics of the cyber warrior. Overall, cyberpower, and in turn mission command, depends upon culturally aware, technically competent and innovative cyber warriors who are equally capable in the joint and coalition environment. As is the case with most, if not all military matters, the people and the leaders make all of the difference.

Conclusion

President Barack Obama, through the Presidential Proclamation of National Cybersecurity Awareness Month (October 2010), stressed that the ―growth and spread of technology" has ―transformed international security and the global marketplace."[44] His statement promised ―if we continue to be a pioneer in innovation and cyber security, we will maintain our strength, resilience, and leadership in the 21st century."[45]

The promise presented by President Obama is clear, as is the reward if that challenge is met. If America can continue to be an innovative pioneer in the cyber domain, she will remain strong and a leader in the 21st century. Coupled with this challenge, our nation also faces an era of persistent conflict in a global environment characterized by failed states, international terrorism, proliferation of weapons of mass destruction (WMD), and the ever-present potential for state-on-state armed conflict.

Armed conflict between sovereign states is nothing new. However, the relatively low cost for aggressive entry into 21st century cyber conflict is very new and presents an additional and unique set of challenges. The cyber domain introduces significant opportunities and likewise exposes potentially critical vulnerabilities of our nation, our military, and our Army. Networks, near real-time data, integrated databases and platforms, firewalls, encryption devices, and smart applications serve as some of the key elements of cyberpower in the 21st century.

The United States depends on capabilities within cyberspace to achieve national objectives in the diplomatic, information, military, and economic elements of national power. According to the 2006 National Military Strategy for Cyberspace Operations, —this reliance provides adversaries a ready avenue of approach to exploit cyberspace to gain strategic, operational, and tactical advantages over the United States."[46] As our nation and our Army becomes increasingly dependent upon control and dominance in the cyber domain, the criticality of the control and security of this domain increases commensurately.

The cyber domain has seen a dramatic evolution and today cyberpower is more than simply enhancing command and control via a more robust and more global communication or information infrastructure.[47] Cyberpower is more than just systems, it is greater than just the unimpeded flow of electrons. Cyberpower rests in the commitment, expertise, determination, and selfless service of our cyber warriors from all

Services, government agencies, coalition partners, and even the civilian sector. According to Lieutenant General Carroll Pollett, Commander of Joint Task Force Global Network Operations and Director of the Defense Information Systems Agency, a new operational criticality is –our ability to deliver decisive capabilities to warfighters and our national leaders…Cyberspace has evolved into a new warfighter domain." LTG Pollett continued by emphasizing that cyberspace has become –just as important as air, sea, land and space as a domain. It's clear that it must be defended and operationalized."[48]

Mission command is linked to cyberpower by its enabling effect. Cyberpower provides the critical transmission layer, consistent and integrated databases containing shared and authoritative data and, and automated analysis and decision tools which enables effective mission command to be realized. The security facet of cyberpower controls access to the cyber domain and defends the legitimacy within the domain.[49]

Mission command is the Army's commander-centric concept which depends upon cyberpower and supporting net-centric, cyber security capabilities. Cyberpower serves as the great enabler for the mission commander at the strategic to tactical level both today and for the future.

Endnotes

[1] Barack Obama, "Presidential Proclamation--National Cybersecurity Awareness Month," October 1, 2010, http://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month (accessed November 4, 2010).

[2] Jay Bavasi, *Fox Business: Biggest National Security Threat: Cyber Attack,* July 26, 2010, http://www.foxbusiness.com/personal-finance/2010/07/26/biggest-national-security-threat-cyber-attack/ (accessed January 12, 2011).

[3] James A. Lewis, –Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, Washington, DC, 1.

[4] Melissa Hathaway, *Securing Our Digital Future,* May 29, 2009, http://www.whitehouse.gov/CyberReview/ (accessed December 2, 2010).

[5] US Department of Defense, *Quadrennial Defense Review: Operate Effectively in Cyberspace*, February 2010, 37.

[6] Patrick Gorman, "The Road to Cyberpower," Booz Allen Hamilton, February 2010,1.

[7] American Bar Association Standing Committee on Law and National Security, *National Security Threats in Cyberspace Workshop Report*, 2009,1.

[8] Bavasi, *Fox Business: Biggest National Security Threat: Cyber Attack,* 1.

[9] Robert Ogilvie, "The Birth of the Auftragstaktik and Its Meaning For the Modern Enterprise," *Ezine Articles,* March 17, 2009, http://ezinearticles.com/?The-Birth-of-the-Auftragstaktik-and-Its-Meaning-For-the-Modern-Enterprise&id=2111060 (accessed October 27, 2010).

[10] Ibid.

[11] Richard N. Pedersen, "Mission Command — A Multifaceted Construct." *Small Wars Journal*, November 17, 2010, 1.

[12] Ibid, 2.

[13] United States Army Training and Doctrine Command (TRADOC), *TRADOC Pamphlet 525-3-3 The United States Army Functional Concept for Mission Command 2010*, 14.

[14] Ivan Yardley, "What is Mission Command?" *Business Command Blog,.* October 18, 2010, http://www.businesscommand.co.uk/about.php (accessed December 10, 2010).

[15] Ibid.

[16] United States Army Training and Doctrine Command (TRADOC), *TRADOC Pamphlet 525-3-3 The United States Army Functional Concept for Mission Command 2010*, 14.

[17] Pedersen, "Mission Command — A Multifaceted Construct." *Small Wars Journal*, 1.

[18] Carroll Kim, "TRADOC leaders provide mission command update at conference," *.* October 26, 2010, http://www.army.mil/-news/2010/10/26/47203-tradoc-leaders-provide-mission-command-update-at-conference/index.html (accessed December 4, 2010).

[19] FM 6-0 Mission Command ." Washington, DC: Department of the Army, August 11, 2003.

[20] *TRADOC PAM 525-3-3 The United States Army Functional Concept for Mission Command.* US Army, 15.

[21] Pedersen, "Mission Command — A Multifaceted Construct," 2.

[22] Martin Dempsey, "Mission Command," *Army Magazine*, January 2011.

[23] Don Vandergriff, "Culture to support Mission Command," August 6, 2010, http://donvandergriff.wordpress.com/2010/08/06/culture-to-support-mission-command/ (accessed October 27, 2010).

[24] United States Army, Army *Field Manual 7-30, Chapter 3 (Battle Command)*.

[25] Robert A. Miller, "Protecting our Cyber Borders," *Defense Horizons*, 2010.

[26] Chairman Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, Washington DC, 2006.

[27] US Department of Defense, Quadrennial Defense Review: Operate Effectively in Cyberspace, 38.

[28] Jim Garamone, "Policy official notes cybersecurity challenges (from *The Official Web site of the United States Air Force),"* May 13, 2010, http://www.af.mil/news/story.asp?id=123204343 (accessed December 16, 2010).

[29] Hathaway, *Securing Our Digital Future.*

[30] Siobhan Gorman, "Military Command Is Created for Cyber Security," Wall Street Journal*,* June 24, 2009, http://online.wsj.com/article/SB124579956278644449.html (accessed January 9, 2011).

[31] Jim Garamone, *Cybersecurity Must Balance 'Need to Know' and 'Need to Share',* December 9, 2010, http://www.defense.gov/news/newsarticle.aspx?id=62040 (accessed January 10, 2011).

[32] Nicholas Hoover, *Homeland Security, Defense Sign Cybersecurity Pact,* October 14, 2010. http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=227800034 (accessed January 17, 2011).

[33] Department of Defense, "U.S. Cyber Command Fact Sheet," May 25, 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf (accessed November 22, 2010).

[34] Ibid.

[35] Michael J. Carden, "Cyber Task Force Passes Mission to Cyber Command," September 7, 2010, http://www.defense.gov/news/newsarticle.aspx?id=60755 (accessed 23 November 2010).

[36] Www.army.mil , "Army establishes Army Cyber Command," October 1, 2010, http://www.army.mil/-news/2010/10/01/46012-army-establishes-army-cyber-command/ (accessed January 15, 2011).

[37] Program Manager Battle Command, "Strategic Battle Commmand," 2010, http://peoc3t.monmouth.army.mil/battlecommand/bc_SBC.html (accessed November 23, 2010).

[38] Ibid.

[39] Ibid.

[40] Defense Update, *WIN-T -Warfighter's Information Network – Tactical,* 2009, http://defense-update.com/products/w/win-t.htm (accessed December 15, 2010).

[41] Ibid.

[42] Kris Osborn, "U.S. Army Working to Ramp up Cybersecurity Efforts," *Defense News*, November 20, 2010.

[43] Toni Bowers, "The U.S. needs cyberwarriors," *TechRepublic*, July 26, 2010.

[44] Barack Obama, "Presidential Proclamation--National Cybersecurity Awareness Month."

[45] Barack Obama, "Presidential Proclamation--National Cybersecurity Awareness Month."

[46] Chairman Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, Washington, DC, 2006.

[47] US Department of Defense*, Quadrennial Defense Review: Operate Effectively in Cyberspace, 38*..

[48] US Department of Defense, "Cyber Task Force Passes Mission to Cyber Command," September 9, 2010, http://www.defencetalk.com/cyber-task-force-passes-mission-to-cyber-command-28636/ (accessed December 15, 2010).

[49] David Kuipers, *Control Systems Cyber Security (*Idaho Falls, Idaho: Idaho National Laboratory), 2006.